Docket No.: E005-4000 PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Wann	:	
Serial No. 09/704,769	:	Group Art Unit: 2137
Confirm. No.: 4376	:	Examiner: Paul E. Callahan
Filed: November 3, 2000	:	

For: CRYPTOGRAPHIC DEVICE

APPEAL BRIEF IN COMPLIANCE WITH 37 CFR 41.37

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The Appellant respectfully submits this Appeal Brief in response to the non-final Office Action dated June 3, 2005. In this office action, claims 7-21 were rejected for the second time without having been amended. Accordingly, under 37 CFR 1.191(a) the Appellant is entitled to appeal the rejections in the June 3, 2005 Office Action to the Honorable Board of Appeals of the U.S. Patent and Trademark Office. A Notice of Appeal was filed on September 2, 2005. In compliance with 37 CFR 41.37, this Appeal Brief has the following sections:

(1) Real Party of Interest

(2) Related Appeals and Interferences

(3) Status of Claims

(4) Status of Amendments

(5) Summary of Claimed Subject Matter

(6) Grounds of Rejection to be Reviewed on Appeal

(7) Argument

In compliance with 37 CFR 41.37, this Appeal Brief contains a Claims Appendix. Additionally, the Appellant is unaware of any documents in support of Evidence Appendix and Related Proceedings Appendix.

SECTION (1): REAL PARTY OF INTEREST

The real party of interest is Enova Technology Corp. of Taipei, Taiwan, Republic of China.

SECTION (2): RELATED APPEALS AND INTERFERENCES

The Appellant is unaware of any related Appeals or Interferences relating to the above-referenced patent application.

SECTION (3): STATUS OF CLAIMS

The following is the status of all of the claims:

(a) Claims 1-6 have been cancelled.

(b) Claims 7-32 are rejected and appealed.

SECTION (4): STATUS OF AMENDMENTS

No amendments have been filed since the non-final Office Action mailed June 3, 2005.

SECTION (5): SUMMARY OF CLAIMED SUBJECT MATTER

The present invention is generally directed to a cryptographic device adapted to perform data encryption and decryption on at least one data stream flowing between at least one data generating device and at least one data storage device without compromising overall system performance (Page 3, lines 23-26, of Preliminary Amendment under 37 CFR 1.115 submitted on October 21, 2003). In one embodiment of the present invention, the cryptographic device is adapted to intercept at least one data stream flowing between the data generating device and the data storage device, and transparently perform data encryption and decryption in accordance with the intercepted data stream. (Page 3, lines 30-34, of Preliminary Amendment under 37 CFR 1.115 submitted on October 21, 2003). In another embodiment of the present invention, the cryptographic device comprises a data stream interceptor, a main controller receiving input from the data stream interceptor, a data generating controller adapted to perform at least one data transfer protocol with the data generating device on command from the main controller, a data storage controller adapted to perform at least one data transfer protocol with the data storage device on command form the main controller, and a cipher engine adapted to transparently encrypt and decrypt data streams flowing between the data generating device and the data storage device on command from the main controller. (Page 4, lines 1-8, of Preliminary Amendment under 37 CFR 1.115 submitted on October 27, 2003; also refer to Fig.4 identified in Exhibit B attached to the Preliminary Amendment under 37 CFR 1.115 submitted on October 21, 2003).

SECTION (6): GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 7-32 are currently pending in the above-referenced patent application. The following are the grounds of rejections that are being appealed from the non-final Office Action mailed June 3, 2005:

Issue 1 Claims 7-10 were rejected under 35 U.S.C. 102(a) as being anticipated by Harrison et al. (U.S. Patent No. 6,081,895). However, unlike the recitations of claims 7-10, there is no disclosure in Harrison et al. of "...at least one data stream interceptor..."

Issue 2 Claims 11-21 were rejected under 35 U.S.C. 102(a) as being anticipated by Harrison et al. (U.S. Patent No. 6,081,895). However, unlike the recitations of claims 11-21, there is no disclosure in Harrison et al. of "...at least one data stream interceptor..."

Issue 3 Claims 22-26 and 28-29 were rejected under 35 U.S.C. 102(b) as being anticipated by van Rumpt et al. (U.S. Patent No. 5,513,262). However, unlike the recitations of claims 22-26 and 28-29, there is no disclosure in van Rumpt et al. that "...intercepted data is either encrypted or decrypted or unchanged at the data security apparatus in accordance with a predetermined communication protocol..."

Issue 4 Claim 32 was rejected under 35 U.S.C. 102(b) as being anticipated by van Rumpt et al. (U.S. Patent No. 5,513,262). However, unlike the recitations of claim 32, there is no disclosure in van Rumpt et al. that "...intercepted data is either encrypted or decrypted or unchanged at the data security apparatus in accordance with a predetermined communication protocol..."

Issue 5 Claims 27, 30, and 31 were rejected under 35 U.S.C. 103(a) as being unpatentable over van Rumpt et al. However, unlike the recitations of claims 27, 30, and 31, there is no disclosure in van Rumpt et al. that "...intercepted data is either encrypted or decrypted or unchanged at the data security apparatus in accordance with a predetermined communication protocol..."

SECTION (7): ARGUMENTS

Issue 1 Claims 7-10 were rejected under 35 U.S.C. 102(a) as being anticipated by Harrison et al. (U.S. Patent No. 6,081,895). However, unlike the recitations of claims 7-10, there is no disclosure in Harrison et al. of "...at least one data stream interceptor..."

To establish a *prima facie* case of anticipation under 35 U.S.C. § 102, a single prior art reference must describe each and every element as set forth in the subject claim. *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). "The identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). Also see M.P.E.P. § 2131.

Claims 7-10 recite "...at least one data stream interceptor..."

Harrison et al. relates to a "method and system for managing data unit processing", as specified in the title. On page 3 of the June 3, 2005 Office Action, it is asserted on page 3, lines 3-4 that "...at least one data stream interceptor..." is taught by Harrison et al. in the abstract. Specifically, the Office Action identifies the disclosure in the abstract of "a channel for processing data units" as teaching "at least one data stream interceptor".

However, "a channel for processing data units" disclosed in Harrison et al. is not "at least one data stream interceptor" as recited in claims 7-10. Accordingly, the recitations in claims 7-10 of "at least one data stream interceptor" are not described in

Harrison et al. At least for this reason, a *prima facie* case of anticipation under 35 U.S.C. § 102 has not been established, since the single prior art reference of Harrison et al. does not describe each and every element as set forth in claims 7-10. *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987).

Issue 2 Claims 11-21 were rejected under 35 U.S.C. 102(a) as being anticipated by Harrison et al. (U.S. Patent No. 6,081,895). However, unlike the recitations of claims 11-21, there is no disclosure in Harrison et al. of "...at least one data stream interceptor..."

The requirements to establish a *prima facie* case of anticipation under 35 U.S.C. § 102 are describe in Issue 1 above.

Claims 11-21 recite "...at least one data stream interceptor..."

Harrison et al. relates to a "method and system for managing data unit processing", as specified in the title. On page 3 of the June 3, 2005 Office Action, it is asserted on page 3, lines 3-4 that "...at least one data stream interceptor..." is taught by Harrison et al. in the abstract. Specifically, the Office Action identifies the disclosure in the abstract of "a channel for processing data units" as teaching "at least one data stream interceptor".

However, "a channel for processing data units" disclosed in Harrison et al. is not "at least one data stream interceptor" as recited in claims 11-21. Accordingly, the recitations in claims 11-21 of "at least one data stream interceptor" are not described in Harrison et al. At least for this reason, a *prima facie* case of anticipation under 35 U.S.C. § 102 has not been established, since the single prior art reference of Harrison et al. does not describe each and every element as set forth in claims 11-21. *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987).

Issue 3 Claims 22-26 and 28-29 were rejected under 35 U.S.C. 102(b) as being anticipated by van Rumpt et al. (U.S. Patent No. 5,513,262). However, unlike the recitations of claims 22-26 and 28-29, there is no disclosure in van Rumpt et al. that "...intercepted data is either encrypted or decrypted or unchanged at the data security apparatus in accordance with a predetermined communication protocol..."

The requirements to establish a *prima facie* case of anticipation under 35 U.S.C. § 102 are describe in Issue 1 above.

Claims 22-26 and 28-29 recite "...intercepted data is either encrypted or decrypted or unchanged at the data security apparatus in accordance with a predetermined communication protocol..."

van Rumpt et al. relates to a "device for enciphering and deciphering, by means of the DES algorithm, data to be written to be read from a hard disk", as specified in the title. It is asserted on page 4 of the June 3, 2005 Office Action that the recitations of "...intercepted data is either encrypted or decrypted or unchanged at the data security apparatus in accordance with a predetermined communication protocol..." are disclosed in van Rumpt et al. in column 2, lines 45-50. However, column 2, lines 45-50 merely disclose:

> "The cipher unit 25 is of a current commercially available type, for instance one of the types supplied by the firm of Western Digital. Since the actual operation of the DES cipher algorithm is not important for a proper understanding of the present invention, except that it is necessary to know that encryption occurs word for word using the, 56-bit encryption key and that the words have a width of 64 bits, the operation of this algorithm will not be further explained."

However, this disclosure in van Rumpt et al. does not relate to a dependency on how data is handled (e.g. encryption, decryption, or unchanged) based on a communication protocol. Accordingly, the disclosure in column 2, lines 45-50, does not anticipate the recitations in claims 22-26 and 28-29 that "...intercepted data is either encrypted or decrypted or unchanged at the data security apparatus in accordance with a predetermined communication protocol..." At least for this reason, a *prima facie* case of anticipation under 35 U.S.C. § 102 has not been established, since the single prior art reference of van Rumpt et al. does not describe each and every element as set forth in claims 22-26 and 28-29. *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987).

Issue 4 Claim 32 was rejected under 35 U.S.C. 102(b) as being anticipated by van Rumpt et al. (U.S. Patent No. 5,513,262). However, unlike the recitations of claim 32, there is no disclosure in van Rumpt et al. that "...intercepted data is either encrypted or decrypted or unchanged at the data security apparatus in accordance with a predetermined communication protocol..."

The requirements to establish a *prima facie* case of anticipation under 35 U.S.C. § 102 are describe in Issue 1 above.

Claim 32 recites "...intercepted data is either encrypted or decrypted or unchanged at the data security apparatus in accordance with a predetermined communication protocol..."

van Rumpt et al. relates to a "device for enciphering and deciphering, by means of the DES algorithm, data to be written to be read from a hard disk," as specified in the title. It is asserted on page 4 of the June 3, 2005 Office Action that the recitations of "...intercepted data is either encrypted or decrypted or unchanged at the data security apparatus in accordance with a predetermined communication protocol..." are disclosed in van Rumpt et al. in column 2, lines 45-50. However, column 2, lines 45-50 merely disclose:

> "The cipher unit 25 is of a current commercially available type, for instance one of the types supplied by the firm of Western Digital. Since the actual operation of the DES cipher algorithm is not important for a proper understanding of the present invention, except that it is necessary to know that encryption occurs word for word using the, 56-bit encryption key and that the words have a width of 64 bits, the operation of this algorithm will not be further explained."

However, this disclosure in van Rumpt et al. does not relate to a dependency on how data is handled (e.g. encryption, decryption, or unchanged) based on a communication protocol. Accordingly, the disclosure in column 2, lines 45-50, does not anticipate the recitations in claim 32 that "...intercepted data is either encrypted or decrypted or unchanged at the data security apparatus in accordance with a predetermined communication protocol..." At least for this reason, a *prima facie* case of anticipation under 35 U.S.C. § 102 has not been established, since the single prior art reference of van Rumpt et al. does not describe each and every element as set forth in claim 32. *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987).

Issue 5 Claims 27, 30, and 31 were rejected under 35 U.S.C. 103(a) as being unpatentable over van Rumpt et al. However, unlike the recitations of claims 27, 30, and 31, there is no disclosure in van Rumpt et al. that "...intercepted data is either encrypted or decrypted or unchanged at the data security apparatus in accordance with a predetermined communication protocol..."

To establish a *prima facie* case of obviousness under 35 U.S.C. § 103, three basic criteria must be met. First, the prior art reference (or references when combined) must teach or suggest all the claim limitations. Second, there must be some suggestion or motivation in the references themselves to modify the reference or to combine reference teachings. Third, there must be a reasonable expectation of success for the modification or combination of references. The teaching or suggestion to make the modification or combination of prior art and the reasonable expectation of success must both be found in the prior art, and not based on Applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). There must be particular findings as to the specific understanding or principle within the knowledge of a skilled artisan that would have motivated one with no knowledge to the claimed invention to combine or modify references. *In re Kotzab*, 217 F.3d 1365, 55 U.S.P.Q.2d 1313 (Fed. Cir. 2000). Conclusory statements cannot be relied up for particular combinations of prior art and specific claims. *In re Lee* 277 F.3d 1338, 61U.S.P.Q.2d 1430 (Fed. Cir. 2002).

Claims 27, 30, and 31 recite "...intercepted data is either encrypted or decrypted or unchanged at the data security apparatus in accordance with a predetermined communication protocol..."

van Rumpt et al. relates to a "device for enciphering and deciphering, by means of the DES algorithm, data to be written to be read from a hard disk", as specified in the title. It is asserted on page 4 of the June 3, 2005 Office Action that the recitations of "...intercepted data is either encrypted or decrypted or unchanged at the data security apparatus in accordance with a predetermined communication protocol..." are disclosed in van Rumpt et al. in column 2, lines 45-50. However, column 2, lines 45-50 merely disclose:

> "The cipher unit 25 is of a current commercially available type, for instance one of the types supplied by the firm of Western Digital. Since the actual operation of the DES cipher algorithm is not important for a proper understanding of the present invention, except that it is necessary to know that encryption occurs word for word using the, 56-bit encryption key and that the words have a width of 64 bits, the operation of this algorithm will not be further explained."

However, this disclosure does not relate to a dependency on how data is handled (e.g. encryption, decryption, or unchanged) based on a communication protocol. Accordingly, the disclosure in column 2, lines 45-50, does not disclose the recitations in claims 27, 30, and 31 that "...intercepted data is either encrypted or decrypted or unchanged at the data security apparatus in accordance with a predetermined communication protocol..." At least for this reason, a *prima facie* case of obviousness under 35 U.S.C. § 103 has not been established, since the cited prior art reference of van Rumpt et al. does not teach or suggest all the claim limitations in claims 27, 30, and 31.

CONCLUSION

In view of the foregoing, it is respectfully submitted that the rejections of claims 7-32 should be withdrawn by the Honorable Board of Appeals and the above-referenced patent application should issue as a patent. The Honorable Board of Appeals is invited to contact the undersigned attorney, **Daniel H. Sherr** or **Natu Patel**, at the telephone number listed below, if any issues arise.

Respectfully submitted,
THE PATEL LAW FIRM, P.C.

Natu J. Patel
Registration No. 39,559

2532 Dupont Drive
Irvine, CA 92612
(949) 955-1077

CLAIMS APENDIX

7. A cryptographic device, comprising:

at least one data stream interceptor;

a main controller receiving input from said at least one data stream interceptor;

at least one data generating controller adapted to perform at least one data transfer protocol with at least one data generating device on command from said main controller;

at least one data storage controller adapted to perform at least one data transfer protocol with at least one data storage device on command from said main controller; and

at least one cipher engine adapted to transparently encrypt at least one data stream flowing between said at least one data generating device and said at least one data storage device on command from said main controller.

8. The cryptographic device of claim 7, wherein said at least one cipher engine is operatively coupled between at least one input buffer and at least one output buffer.

9. The cryptographic device of claim 8, wherein said at least one input buffer receives data from said at least one data generating device and said at least one data storage device.

10. The cryptographic device of claim 8, wherein said at least one output buffer outputs data to said at least one data generating device and said at least one data storage device.

11. A cryptographic device, comprising:

at least one data stream interceptor;

a main controller receiving input from said at least one data stream interceptor;

at least one data generating controller adapted to perform at least one data transfer protocol with at least one data generating device on command from said main controller;

at least one data storage controller adapted to perform at least one data transfer protocol with at least one data storage device on command from said main controller; and

at least one cipher engine adapted to transparently decrypt at least one data stream flowing between said at least one data generating device and said at least one data storage device on command from said main controller.

12. The cryptographic device of claim 11, wherein said at least one cipher engine is operatively coupled between at least one input buffer and at least one output buffer.

13. The cryptographic device of claim 12, wherein said at least one input buffer receives data input from said at least one data generating device and said at least one data storage device.

14. The cryptographic device of claim 12, wherein said at least one output buffer outputs data to said at least one data generating device and said at least one data storage device.

15. The cryptographic device, comprising:

at least one data stream interceptor;

a main controller receiving input from said at least one data stream interceptor;

at least one data generating controller adapted to perform at least one data transfer protocol with at least one data generating device on command from said main controller;

at least on data storage controller adapted to perform at least one data transfer protocol with at least one data storage device on command from said main controller; and

at least one cipher engine adapted to transparently encrypt and decrypt at least one data stream flowing between said at least one data generating device and said at least one data storage device on command from said main controller.

16. The cryptographic device of claim 15, wherein said at least one cipher engine is operatively coupled between at least one input buffer and at least one output buffer.

17. The cryptographic device of claim 16, wherein said at least one input buffer receives data from said at least one data generating device and said at least one data storage device.

18. The cryptographic device of claim 16, wherein said at least one output buffer outputs data to said at least one data generating device and said at least one data storage device.

19. A cryptographic device operatively coupled between a data generating device and a data storage device for use during data transfer, said cryptographic device comprising:

a data steam interceptor;

a main controller receiving input from said at least one data stream interceptor;

a data generating controller adapted to perform at least one data transfer protocol with the data generating device on command from said main controller;

a data storage controller adapted to perform at least one data transfer protocol with the data storage device on command from said main controller; and

a cipher engine adapted to transparently encrypt and decrypt at least one data stream flowing between the data generating device and the data storage device on command from said main controller.

20. A cryptographic device integrated within a data storage device for use during data transfer with a data generating device, said cryptographic device comprising:

a data stream interceptor;

a main controller receiving input from said data stream interceptor;

a data generating controller adapted to perform at least one data transfer protocol with the data generating device on command from said main controller;

a data storage controller adapted to perform at least one data transfer protocol with the data storage device on command from said main controller; and

a cipher engine adapted to transparently encrypt and decrypt at least one data stream flowing between the data generating device and the data storage device on command from said main controller.

21. A cryptographic device integrated within a data generating device for use during data transfer with a data storage device, said cryptographic device comprising:

a data stream interceptor;

a main controller receiving input from said data stream interceptor;

a data generating controller adapted to perform at least one data transfer protocol with the data generating device on command from said main controller;

a data storage controller adapted to perform at least one data transfer protocol with the data storage device on command from said main controller; and

a cipher engine adapted to transparently encrypt and decrypt at least one data stream flowing between the data generating device and the data storage device on command from said main controller.

22. An apparatus comprising a data security apparatus configured to intercept data that is either transmitted from or to be received by a data processing apparatus, wherein:

intercepted data is either encrypted or decrypted or unchanged at the data security apparatus in accordance with a predetermined communication protocol; and

the data processing apparatus operates independently from the data security apparatus.

23. The apparatus of claim 22, wherein the data security apparatus is configured to interface with a data storage apparatus.

24. The apparatus of claim 23, wherein the intercepted data is transmitted from or to be received by the data storage apparatus.

25. The apparatus of claim 23, wherein the data storage apparatus is selected from a group consisting of:

a hard disk apparatus;

a floppy disk apparatus;

a CD apparatus;

a magnetic tape apparatus;

a CD-RW apparatus;

a magnetic optical apparatus;

a digital video recorder;

a flash memory apparatus; and

a PCMCIA apparatus.

26. The apparatus of claim 23, wherein the data storage apparatus is permanently coupled to the data security apparatus.

27. The apparatus of claim 23, wherein the data storage apparatus is temporarily coupled to the data security apparatus.

28. The apparatus of claim 22, wherein the data processing apparatus is a central processing unit.

29. The apparatus of claim 28, wherein the central processing unit is comprised in a computing device, wherein the computing device is selected from a group consisting of:

a host computer;

a notebook;

a microprocessor;

a router; and

an interface card.

30. The apparatus of claim 22, wherein the predetermined communication protocol is determined by a control signal from the data processing apparatus.

31. The apparatus of claim 30, wherein the control signal is generated in the data processing apparatus for interpretation at a data storage apparatus.

32. A method comprising intercepting data at a data security apparatus that is either transmitted from or to be received by a data processing apparatus, wherein:

intercepted data is either encrypted or decrypted or unchanged at the data security apparatus in accordance with a predetermined communication protocol; and

the data processing apparatus operates independently from the data security apparatus.

EVIDENCE APPENDIX

None

RELATED PROCEEDINGS APPENDIX

None